Docket No.: 002964.P019
Express Mail No.: EV339917105US

UNITED STATES PATENT APPLICATION

FOR

ENHANCING MESSAGING SERVICES USING TRANSLATION GATEWAYS

Inventors:

Leo A. D'Angelo
Kamran Izadpanah
John J. Bell

Prepared by:
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025
(310) 207-3800

ENHANCING MESSAGING SERVICES USING TRANSLATION GATEWAYS

[0001] This application claims the benefit of the earlier U.S. filing date of Provisional Application No. 60/419,166, filed October 16, 2002.

Background

[0002] An embodiment of the invention relates to the field of messaging through circuit and packet data networks. Specifically, systems, methods and processes for identification, authentication, routing, delivery of electronic messages across one or more communication networks and transmission methods, are described here. These messages may be, but are not limited to, facsimile, voice messages, images, electronic documents, and software elements.

[0003] A provider of unified messaging services may have the following capabilities for servicing the messaging needs of its customers. First, each customer is assigned a unique telephone number. The customer can give this number to others; the others can then leave messages for the customer at that number (*e.g.*, voice and facsimile messages). The way these messages are processed and stored may be as follows. A network of servers, which can be owned and/or managed by the service provider, is configured to capture an inbound message that has been transmitted to the customer's phone number over the public switched telephone network (PSTN). Once captured, typically in digital form, the message is then sent, as an attachment to an email message, to the customer's email address. This is the address of an email box that typically will have been previously established by the customer; the customer would have reported his email address to the service provider. The customer can now retrieve the messages, by accessing her email box, detaching and then viewing or playing back the attached messaged. This technique for unified messaging has a number of advantages for the customer, including a single interface for retrieving different types of messages, and a relatively inexpensive storage area for her messages.

[0004] The provider's server network can span different cities, states, and countries, so customers may be assigned telephone numbers over a wide geographical range. Thus, a customer living in New York City may request a telephone number that has a New York City area code. A server in that area code can then be configured to recognize incoming calls to that customer's telephone number, capture the inbound message and then address the message (via an email attachment, for example) to the customer's data network address. A central database managed by the service provider and accessible by all of the servers (in the service provider's network), can be used to associate each customer's phone number with his data network address and his message forwarding instructions (such as the file format of the email attachment). The server uses the database to determine where to route the message for a particular customer, i.e. which node of the provider's network can most cost efficiently forward the message, or which node has the needed resource to translate the message into a certain format required by the customer's machine.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The invention is illustrated by way of example and not by way of limitation in the figures of the accompanying drawings in which like references indicate similar elements. It should be noted that references to "an" embodiment of the invention in this disclosure are not necessarily to the same embodiment, and they mean at least one.

[0006] **Fig. 1** illustrates a block diagram of a network environment in which a messaging service according to one or more embodiments of the invention may be implemented.

[0007] **Fig. 2** illustrates a table of information that may be used by a translation gateway, for routing inbound messages to corporate subscribers.

[0008] **Figs. 3A** and **3B** depict a network environment where the messaging service provides security services on a per connection basis.

[0009] **Figs. 4A** and **4B** show an environment where the messaging service provides security services in the form of encryption on a per message basis.

[0010] **Fig. 5** illustrates a block diagram of an environment for implementing a secure messaging service, using SMTP over SSL.

[0011] **Fig. 6** is a block diagram of an environment for implementing a secure messaging service suitable for individual subscribers.

DETAILED DESCRIPTION

[0012] Techniques are described for the communication of messages between a circuit switched network such as a telephone network and a packet switch network (also referred to as a data network). The transfer of messages is enhanced by using translation gateways at the edge of the data networks. The translation gateway may be designed to provide one or more translation functions that are performed upon messages, to for example provide security services between the sender and recipient over a hostile data network. In addition, the architecture involving translation gateways allows the environment or system as a whole to scale more easily as the number of subscribers or customers increase. Such subscribers and customers are those who are under contract with a service provider to pay for the security services used in delivery of their messages. Several embodiments of the invention are now described using voice mail and fax mail messages. However, the translation gateways as well as the methodology described here may be modified to work with other types of electronic messages.

[0013] Beginning with **Fig. 1**, this figure illustrates a block diagram of a network environment in which a messaging service according to one or more embodiments of the invention may be implemented. The network environment is divided into several different networks. First, a unified messaging service provider (UMSP) network 110 is a data network of different types of resources that may be owned and administered by a service provider entity, such as the assignee of this application namely j2 Global Communications, Inc. of Hollywood, California. For example, the UMSP network 110 may be one in which Internet Protocol (IP) addresses for the nodes of the network are assigned by an administrator that is an employee of the service provider. In addition, the UMSP network 110 is a private network in that it has a security barrier against unauthorized access to its nodes and its content. The UMSP network 110 may also be viewed as a globally distributed interface to a circuit switched network 160 (also referred to as the public switched telephone network, PSTN, or telephony network). The UMSP network 110 has resources that can capture inbound messages that originate or

pass through the circuit switched network 160, as well as transmit outbound messages through the circuit switched network 160. A source of the inbound message may be a conventional facsimile machine 170 or a computer (not shown) with facsimile capability, and any type of telephone unit 171. These devices may also be used as the ultimate recipient of outbound messages, for example via telephone calls dialed by a resource of the UMSP network 110.

[0014] The ultimate destination of an inbound message may be a client software program running in a notebook computer 180, where the client process and in this case notebook computer 180 are owned or administered by a subscriber or customer of the messaging service. This subscriber may be an individual, or it may be an organization such as a company that has paid the service provider for the messaging service to be used by a number of its employees or affiliates. In the embodiment shown in **Fig. 1**, the subscriber has or administers a customer network 150 which is a packet-switched or data network that may also be considered private in that unauthorized access to its nodes and content is prohibited. The customer network 150 may be as small as a single local area network (LAN) or it may be made of multiple networks connected to each other to form a wide area or enterprise network.

[0015] Putting the customer network 150 in communication with the UMSP network 110 is a hostile data network 130, such as the public Internet. Data network 130 is deemed hostile because messages that are transferred through that network are not guaranteed any form of privacy. Nevertheless, the data network 130 may be used as an efficient means for communicating messages between the customer network 150 and the UMSP network 110 over a wide geographic area, as described here.

[0016] At the edge of the customer network 150, and therefore considered to be a node of the customer network 150, is a translation gateway 141. In this embodiment, there is also another translation gateway 120 that is a node of and is on the edge of the UMSP network 110. Each of these translation gateways has a port (in, for example, an application layer or other layer above the network layer of the Open Systems Interconnect Reference Model data network communications protocol) that allows access to the hostile data

network 130. Each gateway 120, 141 has certain translation functions that as described here enhance the messaging service provided to the subscribers. The translation gateway may thus be viewed as a protocol converter. An example of policy-based secure message delivery software that can be used to implement some of the functionality of the translation gateways 120, 141 is the MMS SECURE REDIRECT solution by Tumbleweed Communications, Corp., Redwood City, California.

[0017] The translation gateways 120, 141 are capable of sending and receiving inbound and outbound messages using standard network protocols, such as simple mail transfer protocols (SMTP) which is a protocol for sending email messages between servers. Email messages can then be retrieved with an email client program that uses either the post office protocol (POP) or Internet message access protocol (IMAP). Another communications protocol that may be used to transfer messages between a translation gateway and another node is web-based distributed authoring and versioning (WebDAV) which is a platform independent extension to the hypertext transport protocol (HTTP) that allows users to collaboratively edit and manage files on remote web servers. Yet another communication protocol that may be used is the session initiated protocol (SIP) which is a signaling protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. The protocol is used to initiate call setup, routing, authentication and other feature messages to end points within an IP domain.

[0018] A domain here refers to a group of computers or devices on a network that are administered as a unit, with common rules and procedures. Within the Internet for example, domains are defined by the IP address. All devices sharing a common part of the IP address are said to be in the same domain. A large or corporate customer may register one or more domains in its name.

[0019] A translation gateway in response to receiving a message on a given transport, performs a translation function based on a set of rules that are contained within the message body or are within a configuration script of the gateway itself. Possible translation functions include translation between

protocols (for example from an SMTP format to an instant messaging format, and back), as well as privacy/security which is described below. The gateway translates the message to its intended format or otherwise applies the translation function to the message, and then resends the message to its ultimate recipient. Thus for example in **Fig. 1**, a fax message that has been transmitted by the fax machine 170 is captured by an inbound resource of the UMSP network 110. This was preceded by a telephone call made by the fax machine 170 using the circuit switched network 160, to an inbound telephone number that has been assigned, by the UMSP network administrator or another UMSP agent, to a particular subscriber. This inbound telephone number is used by the subscriber to receive telephone fax or voice mail messages (or both). The UMSP network 110 may allow the subscriber to customize for example an outgoing message that is played back in response to an incoming call.

[0020] Once captured, the inbound message is routed through the UMSP network 110 to the appropriate translation gateway 120. Thus, for example, if the inbound message is on behalf of a particular corporate subscriber, the message is routed to the translation gateway 120 that has been assigned for handling message traffic for that subscriber. See, for example, the look-up table shown in **Fig. 2**. For simplicity, other translation gateways are not shown in **Fig. 1** but may of course be present depending upon how many subscribers the service has and the amount of expected message traffic. The architecture may thus be scaled relatively easily, by simply adding additional translation gateways as the number of subscribers or messages increase. Note also that the message may be converted for example from a fax protocol format into a digital format such as TIFF or PDF, prior to being delivered to the translation gateway 120.

[0021] Upon receiving the inbound message, the translation gateway 120 determines which address to forward the message, using for instance a lookup table such as the one illustrated in **Fig. 2**. The example in **Fig. 2** shows that a set of inbound telephone numbers that has been assigned to the subscriber company A is associated with the domain name *companyA.com*. There may be a different individual user associated with each telephone number as shown, so

that a complete address may be defined as the combination *username@companyA.com*. Such detailed information about the identity of the individual users or their complete, individual addresses, however, need not be present in the translation gateway or in the UMSP network in general, in order for the gateway 120 to do its job of forwarding the messages to the customer network 150 (see **Fig. 1**). The service may thus be operated on a per domain basis, with all inbound messages that arrive on the inbound telephone numbers of a given customer (as determined by the lookup table in **Fig. 2**, for example) being pushed to the corresponding customer's translation gateway network address. It will then be up to the translation gateway 141 to match the correct email address (or other data network address on the customer network 150) to each inbound message, using for instance, the inbound telephone number as an index to a look-up table.

[0022] At the translation gateway 120, forwarding is achieved by for example attaching the message to an email that is addressed to a subscriber's predefined email address (*e.g., smtp@companyA.com*) that has been assigned to the translation gateway 141. The message traverses the hostile data network 130 on its way to the translation gateway 141. Accordingly, an embodiment of the invention is directed to providing the inbound message with privacy as it traverses this hostile data network. This security feature may be provided in different ways, for example either through a secure connection such as a virtual private network tunnel (see **Figs. 3A** and **3B** described below) or encryption on a per message basis such as using the Secure Multipurpose Internet Mail Extensions (S-MIME) protocol (**Figs. 4A** and **4B**) or using SMTP over Secure Sockets Layer (SSL) which runs "on top of" TCP/IP, *i.e.* uses TCP/IP to support application tasks such as displaying web pages or running email servers (see **Fig. 5**).

[0023] Returning to **Fig. 1**, as inbound messages are received over the hostile data network 130 at the translation gateway 141, they may be forwarded to an email server for storage (not shown) from which they can be accessed by a client program running in the notebook computer 180 and which has been configured (with a security certificate that allows access to its user's email box) by an administrator of the customer network. As mentioned above, this client

program may alternatively be running in other types of devices, such as a desktop computer, a personal digital assistant (PDA), a mobile phone unit (not shown) or any type of networked electronic appliance.

[0024] Another embodiment of the invention lies in an outbound service provided to subscribers of the UMSP. The outbound service may be implemented as follows. As part of its contract for secure messaging services, the subscriber is informed, by the service provider, of a domain name such as *secure.outboundservice.com* which represents a domain of outbound resources in the UMSP network 110 that is owned or administered by the service provider. In the embodiment of **Fig. 1**, it is the same translation gateway 120 used for inbound services that is assigned the domain name for outbound service. A client program, such as an email client of the subscriber, may then send an outbound message, in the form of an attachment for example, that is addressed to the domain name. For fax and voice messages in particular, the service provider further instructs the subscriber to add the destination, circuit switched network address (*e.g.*, telephone number) as a prefix (*e.g.*, *13108205988@secure.outboundservice.com*) prior to sending the outbound message. This prefix will then be interpreted by the translation gateway 120, to determine the appropriate outbound resource within the UMSP network 110 that will be able to forward the message to its ultimate destination, namely the indicated telephone number.

[0025] The outbound message is first delivered to the translation gateway 141 via email through the customer network 150. This getaway 141 then determines, through for example a lookup table (not shown), the data network address of the translation gateway 120 belonging to the service provider. In other words, the translation gateway 141 recognizes the mapping between the domain name in the address of the email message and, for example, an IP address of the service provider's translation gateway 120. The message, and in particular the attachment in the case of email, is then sent through the hostile data network 130 while maintaining privacy, and arrives at the translation gateway 120. There, after verifying that the message is from a current subscriber (by, for example, analyzing the "from" field of the email), the translation gateway 120 may determine what is the most efficient manner

of delivering the message to its intended recipient. For example, if the message is intended to be delivered to a facsimile number, then an outbound resource that has a fax telephoning card may be designated to receive the message. If the message is a voice message that is for example an audio or video recording, then a audio or video telephoning card that can relay such a message to the intended recipient is designated to receive the message. Alternatively, the message may be placed into a queue from which messages are pulled, according to their types, by the various outbound resources as these become available to transmit. The message then may be routed through the UMSP network 110 which, as mentioned above, may be a globally distributed network. Thus for example the translation gateway 120 may be located in one country but the outbound resource which places the phone call, for example to transmit the fax or play back the voice message, or otherwise transmits the outbound message, is located in another country.

[0026] Turning now to **Figs. 3A** and **3B**, what is shown is a network environment where the messaging service provides security services on a per connection basis. In this embodiment, a virtual private network (VPN) tunnel is established between predefined ports of the translation gateway 120 and translation gateway 141, for customer B. The VPN tunnel at port X of gateway 120 may be viewed as an extension of customer B's data network 350, while the one at port Y of gateway 121 is an extension of customer A's data network 351. In this embodiment, the gateways actually may be implemented as routers, where the gateways 120 and 141 feature routers that are preferably both administered by customer B, while those in gateways 121, 142 are administered by in this case customer A. Additional VPN tunnels may be established for the benefit of another corporate or institutional subscriber. Data traffic through the VPN tunnels is secure in that as messages are traversing through the data network 130 their privacy, as well as other security features such as integrity, are maintained in the face of attacks. The VPN tunnels may be used for both inbound and outbound messages.

[0027] Note that each of the routers shown in **Fig. 3A** has a unique IP address on the hostile data network 130. After a port is negotiated between two routers, the two routers form a virtual private network with the ability to

communicate messages securely between them, over the hostile data network 130. It should be noted again that the gateway 141 (router for customer B) is a node of customer B's data network 350, but not of the UMSP network 110 (see **Fig. 3B**). Similarly, the router in the translation gateway 142 is a node of customer A's data network 351, but not the UMSP network 110. At the other end of the hostile data network 130, the routers in both gateways 120, 121 are different nodes of both the hostile data network 130 and the UMSP network 110, but not of either customer A's data network 350 or customer B's data network 351.

[0028] As was mentioned above, the messaging service may provide the ability to forward both inbound and outbound messages for its subscribers. As another example, **Fig. 3B** shows a number of devices that can source inbound messages, and receive outbound messages. These devices include a conventional facsimile machine 371, 372, a landline telephone unit 373, 374, a cellular mobile unit 375, and a desktop or notebook computer 377. In this embodiment, all of these devices communicate through the circuit switched network (PSTN) 160. The service provider may contract with local phone companies to lease a number of telephone lines of the circuit switched network 160. Thus, in the example shown in **Fig. 3B**, there are lines leased in New York, Los Angeles, and Chicago. These lines connect the circuit switched network 160 to local phone company switches 380-382. The switches 380-382 are communicatively coupled to notify one or more voice/fax cards 390, that are in respective inbound and outbound servers 392-394, that there is an incoming call to a given inbound address (*e.g.*, telephone number) assigned to a line leased by the service provider. The servers 392-394 are respective nodes of the UMSP network 110.

[0029] A customer information database 396 may also be provided as part of the UMSP network 110, as a central storage for customer account information. Such customer account information would include for example the information shown in the table of **Fig. 2**. In addition, translation options if any for each subscriber may also be included in this database. This database 396 may also be accessed by the translation gateway 120, to determine which translation functions need to be applied to the messages of a particular

subscriber. For example, certain messages may need to be translated from one protocol to another, or from one format to another, prior to being forwarded. Thus, the database 396 may indicate that facsimile messages should be translated into an instant messaging (IM) format for use by a particular client (IM) process 379 (see **Fig. 3A**), rather than by an email client 364. Other customer-specified translation and filtering rules may also be stored in the database 396. Of course, portions of the database 396 may be copied to other elements of the UMSP network within local, cache-type storage units (not shown).

[0030] Still referring to **Fig. 3A**, note that the translation gateway 141 for customer B is configured in this embodiment to recognize that different types of inbound messages through its port X may need to be processed differently. For example, email messages would be forwarded to email server 362 (which may be a separate node of customer B's data network 350), while other types of messages such as instant messaging (IM) would be forwarded to an IM storage area or directly to the client process 379 if the IM client is on line. Other forms of groupware may also be supported by the translation gateway 141, to deliver inbound messages to a predefined client process, or receive outbound messages from certain client processes.

[0031] It should be noted that the above-described embodiments of the messaging service are a for-profit service for which subscribers have agreed to pay on a monthly basis, or some other interval for billing. These secure services may be offered to the subscribers at an additional premium, above a basic set of unified messaging services in which inbound and/or outbound messages are delivered for the subscriber without guaranteeing their privacy or integrity as they traverse a hostile data network. The service provider may provide the subscriber a report or bill for example on a monthly basis that details the charges incurred by the subscriber including the type of service used and how it was used as well as how often it was used.

[0032] Turning now to **Figs. 4A** and **4B**, these show a network environment where inbound messages are delivered securely to corporate subscribers company A and company B using encryption on a per-message

basis. In this embodiment, the translation gateway 120 has a security function that when applied precludes unauthorized access to the content of inbound messages as these are forwarded by the translation gateway 120 through the hostile data network, in this case being the Internet 230, to either translation gateway 141 or 241 (see **Fig. 4B**). Thus, the same translation gateway 120 may be used to apply a security function to messages on behalf of more than one corporate subscriber. The security function in this embodiment is to translate the inbound messages that have been captured by an inbound resource 420 (and which may originate from a conventional fax machine 470) into S-MIME format, and address these encrypted messages to the domain name of the respective customer A or B (previously assigned to the translation gateway 141 or 241). When these encrypted messages are received by the translation gateway 141 or 241, they may be converted into MIME in this embodiment, and then handed off to an email server that is on the data network 452 (and administered by company A), or that is on the data network 454 (administered by company B). These email messages may then be accessed by authorized client processes that are running in for example a personal digital assistant (PDA) 455 or a notebook computer 457, over their respective data networks 452, 454.

[0033] The same translation gateways 141, 241 used for inbound service may also be used for outbound service. A security function may be added by which an outbound email message (sourced from for example the PDA 455 or notebook computer 457) is translated from MIME to S-MIME, after being pulled from the respective email servers 424, 428. For example, all email messages addressed to the domain *secure.outboundservice.com* are pulled from the email server and following the conversion to S-MIME are forwarded through the Internet 230 to the translation gateway 120 (which is assigned to receive all messages addressed to that domain). The translation gateway 120 and the translation gateways 141, 241 had previously exchanged security certificate keys for implementing the S-MIME protocol, to ensure privacy on a per message encryption basis through the Internet 230. For example, a single set of security certificate keys may be exchanged that is applied by the gateway 141 or 241, to encrypt all of its outbound messages addressed to the service

provider's domain at *secure.outboundservice.com*. Note that while the gateway 120 is administered by the service provider, the gateways 141, 241 are preferably administered by the respective subscribers, company A and company B.

[0034] At the translation gateway 120, as the outbound messages are received in S-MIME format, they are verified as being from a current subscriber (*e.g.*, by checking the "from" field in the case of an email message), and are then decrypted and routed to the appropriate outbound resource 421, in the UMSP network 110 (see **Fig. 4A**). Again, as an example, if the outbound message is an email message that has a facsimile attachment (*e.g.*, a word processor file or an image file) and is addressed to *13108205988@secure.outboundservice.com*, then a routing function in the UMSP network 110 will recognize that the outbound resource 421 has a fax transmission card located in the 310 – area code, such that the attachment can be transmitted relatively cheaply as a local, facsimile protocol call made from that fax card to the given number identified in the prefix of the email address.

[0035] Another embodiment of the invention bypasses or avoids the need for a translation gateway 141 that is on the customer network 452 (see **Fig. 4B**). In that case, the translation gateway 120 would still perform the conversion to S/MIME (for inbound messages) and from S/MIME (for outbound messages), for transmission across the Internet 230 of messages on behalf of company A. However, in the inbound case, the S/MIME message is delivered directly to the email server 424 on customer network 452, and then it is the customer's email client software running in the PDA 455 which provides the decryption functionality required for the customer to read the message. In that case, every user or affiliate of company A, on the customer network 452, may be required to obtain a secure certificate, exchange the certificate with the UMSP network 110 and configure their e-mail client to utilize this certificate for reading encrypted messages. The administrative overhead to provide such functionality may be so great for a medium to large customer network (where there are a large number of affiliates that will use the secure messaging service) as to justify the alternative solution of the translation gateway 141.

[0036] Utilizing a translation gateway to provide enhanced messaging functionality may benefit the unified messaging service provider, in the following ways. A large, distributed UMSP network 110 may consist of hundreds if not thousands of devices distributed globally, some for capturing inbound messages (such as voice and facsimile over the PSTN) and others for transmitting outbound messages (again, such as facsimile and voice over the PSTN). By utilizing the translation gateway 120 to provide the translation functions that are applied to inbound and/or outbound messages, additional functionality can be centralized within the UMSP network 110 rather than distributed to every device within the network. This allows the service provider to provide enhanced functionality quickly and cost effectively without requiring a "fork lift upgrade" to the UMSP network 110.

[0037] Referring now to **Fig. 5**, a block diagram of another environment for implementing a secure messaging service is illustrated. In this embodiment, the higher level, data communications protocol used to securely send inbound and outbound messages through the Internet 556 is referred to as a SSL tunnel that connects an email server 524 in company A's internal data network 552, to an email server 564 in the service provider's internal data network 560. The email servers 524, 564 are administered by company A and the service provider, respectively. The inbound and outbound messages are in this embodiment email messages that may be formed in accordance with SMTP and communicated through the Internet 556 "on top of" SSL. This SSL tunnel is implemented by software that allows the encryption of arbitrary TCP connections inside SSL. Thus, the SSL tunnel application may allow one to secure non-SSL aware daemons and protocols (like POP, IMAP, LDAP, etc.) by having SSL tunnel provide the encryption, without requiring changes to the daemon's code.

[0038] In operation, the SSL tunnel is a transient connection that is created when, for example, in the case of an inbound message, the service provider's email server 564 has received an inbound message (including, for example, a facsimile or voice file attachment) that is addressed to the domain of company A. The SSL tunnel application (which may be running in the email server 564) recognizes that the company A domain is handled by company A's

email server 524, and on that basis creates the SSL tunnel by exchanging security information with the email server 524. Of course, a corresponding SSL tunnel application is running in the company A domain, and in particular in the email server 524, so as to complete the negotiation of security information. Once the secure connection has been established, the inbound message, under control of for instance SMTP, is handed to the SSL tunnel program which then "wraps" the inbound message and sends the message through the SSL tunnel to the email server 524. At the email server 524, the SSL wrapper is undone and the message is handed up to the SMTP software component, where the latter makes the inbound message available for access by a client process in company A's internal data network 552. As mentioned above, this inbound message within the email server 524 may now be accessed through a variety of different client processes that may be running in, for example, a PDA 504, a mobile phone unit 508 (with data or text capability, in addition to voice, and the further capability of accessing the internal data network 552 through a wireless data connection), a notebook computer 516, or a desk top computer 520. Such a secure transfer of the inbound message from the service provider's network 560 to a subscriber's network is seamless to the client process.

[0039] Similarly, for outbound messages, as these are collected in the email server 524 of company A's internal data network 552, a SSL tunnel application that may be running in the email server 524 obtains knowledge of these outbound messages that may have been enqueued, and selects one (addressed to the service provider's domain). An SSL wrapper is then applied to the selected outbound message and a SSL tunnel is negotiated with the email server 564 in the service provider's domain. After the outbound message securely arrives at the service provider's domain, the SSL wrapper is undone and the outbound message is enqueued in the email server 564. Software (that may be also running in the email server 564) detects that the outbound message is from company A's domain, and accordingly verifies (through some customer information database, not shown) that the account of company A is current. The outbound message may then be transferred, still using SMTP for example, to any one of the outbound resources 568, 570, and 572 for instance, depending upon which can most efficiently forward the outbound message into the PSTN

580. Following a translation into a format suitable for communication over the PSTN 580, the outbound message is transmitted through any one of telecommunication lines 569, 571, and 573, after having invoked the circuit switch network address of the recipient's receiver, *e.g.* a landline telephone 581, a mobile phone 583, or a fax machine 584. Again, the secure sending of outbound messages from the subscriber's network to that of the service provider is seamless to the subscriber's client process from which the message originated.

[0040] Using the SSL tunnel application, as described above, may also obviate the need for more expensive and more complex software that supports VPN tunnels (**Fig. 3A**), or an S-MIME connection (**Fig. 4A**). Of course, additional software that provides billing information to the customer, including identifying the inbound and outbound messages that were successfully transferred, as well as the total cost to the customer for such services, may also be needed to run in the service provider's internal data network 560, but is not explicitly shown.

[0041] Turning now to **Fig. 6**, this figure is a block diagram of an environment for implementing a secure messaging service that may be particularly suitable for individual subscribers. In this embodiment, inbound messages are provided with privacy as they traverse the Internet 230, as follows. First, the messages are captured by an inbound resource 420, similar to the situation in **Fig. 4A**. The inbound message may originate as an incoming telephoning call made from either a facsimile machine 470 or a telephone unit 472 to the inbound circuit-switched address (here, telephone number) assigned to the subscriber. After the message has been processed into the desired digital format, the inbound message is stored in a message storage server 508 on behalf of the subscriber. The storage server 508 may be a separate node of the UMSP network 110. Next, a messaging application server 510, which is also another node of the UMSP network 110, obtains knowledge of the stored message and will then send a resource locator link (such as Universal Resource Locator, URL) over a hostile data network such as the Internet 230, to a client process actually being used by, or to be used by, a subscriber of the secure messaging service. The messaging application server 510 may be implemented

as a modified version of the secure message delivery technology referred to as IME by Tumbleweed Communications, Corp., Redwood City, California. The client process may be a client program (*e.g.*, email; instant messaging) running in once again for example a desktop computer 514, a notebook computer 516, or other networked data device. The subscriber may then be instructed by the service provider (*e.g.*, via a text prompt that accompanied the link) to invoke this link so as to establish a connection with the UMSP network 110 (and in this embodiment, the messaging application server 510) to securely receive the stored inbound message. The connection may be, for example, a Secure Socket Layer (SSL) connection over which all data being transferred over the Internet 230 to the client process is encrypted for maintaining privacy. Using such a technique, the subscriber may be prompted to login to a secure web site after having invoked its SSL URL, with a password known only to the subscriber and that was previously assigned by the service provider, so that only the subscriber can login to retrieve her inbound messages. In such an embodiment, there is no need for the client process and the messaging application server 510 to exchange security certificates in order to deliver inbound messages to the subscriber.

[0042] It will be appreciated by those skilled in the art that the block diagrams herein represent conceptual views of illustrative circuitry and/or software embodying the principles of the invention. Similarly, it will be appreciated that any flow charts, flow diagrams, pseudocode and the like represent various processes which may be substantially represented in computer readable medium and so executed by a computer or processor, whether or not explicitly shown.

[0043] The functions of the various elements shown in the figures, including functional blocks labeled as "processors" or "servers" may be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software. When provided by a processor, server or computer, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared. Moreover, explicit use of the term "processor", "server", or "computer" should not be construed to refer

exclusively to hardware capable of executing software, and may implicitly include, without limitation, digital signal processor (DSP) hardware, read-only memory (ROM) for storing software, random access memory (RAM), and non-volatile storage. Other hardware and/or software, standard and/or custom, may also be included.

[0044] To summarize, various embodiments of providing enhanced messaging services using translation gateways have been described. In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention as set forth in the appended claims. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.